mula.

Data Processing Agreement in accordance with Art. 28 para. 3 GDPR

Contractor (Processor):

Go Mula GmbH
Colditzstraße 34-36
12099 Berlin
Berlin, Germany

Client (Controller):

xxxx
xxxx
xxxx
xxxx

1 Subject Matter and Duration of the Agreement

1.1 The Contractor shall provide the Client with a platform for merchandise management. In particular, this platform enables the Client to design merchandise articles and manage the dispatch of the articles. The Contractor processes the Client's personal data ("Client Data") on the basis of this contract. The Contractor shall process the personal data for the duration of the main contract on behalf of and only in accordance with the instructions of the Client.

1.2 Details of the scope of services are set out in the main contract.

1.3 The contractually agreed service shall be provided exclusively in a member state of the European Union or in a state party to the Agreement on the European Economic Area. Any transfer of personal Client Data to a country outside the EU/EEA ("third country") may only take place if the special requirements of Art. 44 et seq. GDPR are fulfilled.

1.4 The contract begins with the signing of the main contract and is concluded for an indefinite period. The term and termination of this contract shall be governed by the provisions on the term and termination of the main contract. Cancellation of the main contract shall automatically result in cancellation of this contract. Isolated cancellation of this contract is excluded.

2 Type and Purpose of Processing, Type of Personal Data and Categories of Data Subjects

2.1 Type and purpose of processing:
The Client has the option of uploading personal data of employees or other persons via the platform and then using it for the design and/or dispatch management of the merchandise items. For this purpose, the Contractor collects and stores the personal data and discloses it to external parties (e.g. shipping service providers) on the instructions of the Client. The purpose of the data processing is the provision of the platform and the fulfilment of the services in accordance with the main contract.

Optionally, the Client can also connect an existing system (e.g. HR system) to the platform via an API for the transfer of personal employee data.

On request, the Contractor also offers the option of setting up and operating a web shop through which the Client can offer its merchandise items for sale. The Client determines the design of the shop and the connected payment and shipping service providers within the scope of the options provided.

2.2 Type of personal data:
The Client independently determines which personal Client Data is processed as part of the order. As a rule, the Contractor processes the following personal Client Data to fulfil the services:

- Contact data (name, delivery address, telephone, e-mail);
- Content data for printing on the products (e.g. photos, other information provided);
- Data for automated dispatch (e.g. birthdays, anniversaries, other occasions);
- Technical log data / log data.

If the Contractor operates a web shop as part of the contract, the following additional information is regularly processed:

- Information on the order (e.g. content, time, shipping service selected);
- Information on any credits with which the customer's employees can purchase items;
- Payment information (e.g. payment method, pseudonymised payment data, time of payment).

2.3 Categories of data subjects:
All persons whose personal data is provided or uploaded by the Client as part of the services. As a rule, this concerns

- Employees of the Client
- Interested parties and end customers of the Client

3 Rights and Obligations of the Client

3.1 The Client is solely responsible for assessing the lawfulness of the processing and for safeguarding the rights of the data subjects in accordance with Articles 12 to 22 GDPR. Nevertheless, the Contractor is obliged to forward all such requests to the Client without delay, provided that they are recognisably addressed exclusively to the Client.

3.2 The Client shall inform the Contractor immediately if it discovers errors or irregularities in the examination of the processing results.

3.3 The Client shall be obliged to treat as confidential all knowledge of the Contractor's business secrets and data security measures acquired in the course of the contractual relationship. This obligation shall remain in force even after termination of this contract.

4 Instructions

4.1 The Contractor shall process personal data exclusively within the framework of the agreements made and in accordance with the instructions of the Client, unless the

Contractor is obliged to do so by the law of the Union or the Member States to which the Processor is subject (e.g. investigations by law enforcement or state security authorities); in such a case, the Processor shall notify the Controller of these legal requirements prior to processing, unless the law in question prohibits such notification on grounds of an important public interest (Art. 28 para. 3 sentence 2 lit. a GDPR).

4.2 As a rule, the Client shall issue all orders, partial orders and instructions in writing or in a documented electronic format. Verbal instructions must be confirmed immediately in writing or in a documented electronic format.

4.3 The Contractor shall notify the Client immediately if, in its opinion, an instruction issued by the Client violates statutory provisions. The Contractor shall be entitled to suspend the execution of the relevant instruction until it is confirmed or amended by the person responsible at the Client after review.

5 Obligations of the Contractor

5.1 If a data subject contacts the Contractor directly to exercise their rights under Chapter 3 GDPR (Art. 12 to 23 GDPR), considering Part 2, Chapter 2 BDSG (Sections 32 to 37 BDSG), the Contractor shall forward this request to the Client without delay. The Contractor shall support the Client in a reasonable manner with appropriate technical and organisational measures to comply with its obligation to respond to such requests to exercise the rights of the data subject referred to in Chapter 3 GDPR.

5.2 The Contractor shall assist the Client in complying with the obligations set out in Articles 32 to 36 GDPR, considering the nature of the processing and the information available to the Contractor.

5.3 The Contractor undertakes to maintain confidentiality when processing the Client's personal data in accordance with the contract. This obligation shall continue even after termination of the contract.

5.4 The Contractor warrants that it will familiarise the employees engaged in the performance of the work with the relevant data protection provisions before commencing their work and that it will impose an appropriate obligation of confidentiality on them for the duration of their work and after termination of the employment relationship.

5.5 The Controller and the Contractor shall co-operate with the supervisory authority upon request. In the event of an inspection of the controller by a supervisory authority, the contractor shall provide the controller with the best possible support.

6. Notification Obligations of the Contractor in the Event of Processing Disruptions and Personal Data Breaches

6.1 The Contractor shall notify the Client without delay of any disruptions, inspections and measures taken by the supervisory authority, violations by the Contractor or the persons employed by the Contractor, violations of data protection regulations or the provisions made in the order, and irregularities in the processing of personal data.

6.2 If the Contractor becomes aware of a breach of the protection of personal data within the meaning of Art. 4 No. 12 GDPR regarding the processed Client data ("data protection incident"), it shall notify the Controller immediately and support the Client with any obligations under Art. 33, 34 GDPR.

7 Subcontracting Relationships with Subcontractors

7.1 The Contractor may establish subcontracting relationships with other processors (subcontractors).

7.2 The Contractor shall always inform the Client of any intended change with regard to the involvement of new subcontractors or the replacement of existing subcontractors, giving the Client the opportunity to object to such changes within two weeks. If the Client does not raise any justified objections within two weeks of notification of the change, the change shall be deemed to have been approved by the Client. The Contractor shall draw the Client's attention to the significance of its behaviour at the beginning of the period. In the event of an objection, the Contractor may, at its own discretion, provide the service without the intended change or - if the provision of the service without the intended change is unreasonable for the Contractor - discontinue the service to the Client within two weeks of receipt of the objection and terminate the main contract without notice and with immediate effect.

7.3 Subcontractors in third countries may only be commissioned if the special requirements of Art. 44 et seq. GDPR are fulfilled.

7.4 The Contractor must contractually ensure that the regulations agreed between the Client and the Contractor also apply to subcontractors. The Contractor must oblige the Client to do so before commencing activities by means of a contract or other legal instrument under Union law or the law of the Member State concerned, whereby in particular sufficient guarantees must be provided that the appropriate technical and organisational measures are implemented in such a way that the processing is carried out in accordance with the requirements of the GDPR.

7.5 At the time of commissioning, the Contractor employs the following subcontractors:

- **Deutsche Post AG, Charles-de-Gaulle-Straße 20, 53113 Bonn, Germany**
    - Triggering of shipments via the platform, overview of shipments, shipment tracking

- **Amazon Web Services EMEA, SARL, B 186.284, 38 Avenue John F. Kennedy, L-1855 Luxembourg**
    - RDS database storage for production database and backups

- **Google Cloud EMEA Limited, 368047, 70 Sir John Rogerson's Quay, Dublin 2, Ireland**
    - Storage of backups, data snapshots and submitted collective delivery lists.

- **Mailjet SAS (Global HQ), 4 rue Jules Lefebvre, 75009 Paris, France**
    - Transaction-related email messages

- **Stripe Payments Europe, Limited (SPEL), 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, Ireland**
    - (Optional) Processing of personal and payment data for the processing of shop payments (Stripe Connect)

- **allbranded GmbH, Stahltwiete 21a, 22761 Hamburg, Germany (parent company)**
    - Support in the operation of the platform (in particular provision of IT systems, support in the processing of orders)

8 Technical and Organisational Measures

8.1 A level of protection appropriate to the risk to the rights and freedoms of natural persons affected by the processing shall be ensured for the specific processing on behalf of the controller. The Contractor shall take all measures required in accordance with Art. 32 GDPR. These measures include, in particular, the ability to ensure confidentiality, integrity, availability and resilience of the systems in the long term and to restore the availability of personal data and access to it quickly in the event of a physical or technical incident.

8.2 The Contractor guarantees that it will implement the technical and organisational measures listed in **Annex 1** of this contract before commencing the processing of the Client Data, maintain them for the duration of the processing and, if necessary, adapt them to the state of the art and the risk of the processing.

8.3 If the measures taken by the Contractor do not meet the Client's requirements, the Contractor shall notify the Client immediately.

8.4 The measures taken by the Contractor may be adapted to technical and organisational developments during the course of the contractual relationship but must not fall below the agreed standards. The Contractor must agree significant changes with the Client in documented form (in writing, electronically). Such agreements must be retained for the duration of this contract.

9. Control Rights of the Client

9.1 The Contractor shall grant the Client a right of inspection to check the data processing and compliance with this contract or the respective project order. In particular, the Contractor shall provide the Client with all information required to prove compliance with the obligations set out in this contract and shall enable audits, including inspections, to be carried out. The inspection activities may also be carried out by a third party bound to secrecy, provided that the third party is not a competitor of the Contractor.

9.2 The parties agree that the Client shall carry out a review in accordance with clause 9.1 by instructing the Contractor to submit, at its discretion, a suitable certificate, report or report extracts from independent bodies (e.g. auditor, internal audit, data protection officer, information security officer, data protection auditor or quality auditor) or a suitable certification through an IT security or data protection audit - e.g. in accordance with ISO 27001). In justified exceptions, the Client may carry out independent inspections.

9.3 The Contractor undertakes to support the performance of the inspections. This includes granting all necessary rights of access, information and inspection. The same applies to public inspections by the competent supervisory authority in accordance with the applicable data protection regulations.

9.4 The Client shall inform the Contractor in good time (generally at least four weeks in advance) of all circumstances relating to the performance of the inspection. As a rule, the Client may carry out one inspection per calendar year. This does not affect the Client's right to carry out further inspections in the event of special incidents.

10 Obligations of the Contractor After Completion of the Order

10.1 The Contractor shall be obliged to delete the personal data completely in accordance with data protection regulations (including the copies required for procedural or security reasons) or to return them to the Client after completion of the work or upon termination/ cancellation of the contract - in accordance with the Client's specifications. The same shall also apply to test and scrap material, which must be kept under data protection-compliant lock and key until it is deleted or returned. This shall not apply if there is an obligation to store the personal data under Union law or the law of the Member States.

10.2 Documentation and logs that serve as proof of proper data processing in accordance with the order or statutory retention periods shall be retained beyond the end of the contract in accordance with the respective retention periods.

11. Final Provisions

11.1 Should individual provisions of this contract be invalid or unenforceable or become invalid or unenforceable after the conclusion of the contract, this shall not affect the validity of the remainder of the contract. Amendments or additions to the contract must be recorded in writing.

11.2 Insofar as no special provisions are contained in this contract, the provisions of the main contract shall apply. In the event of contradictions between this contract and provisions from other agreements, in particular from the main contract, the provisions from this contract shall take precedence.

Signatures

Berlin, xx.xx.xxxx
Go Mula GmbH

Berlin, xx.xx.xxxx
xxxxxxxx

Attachments:

- Annex 1: Technical and Organisational Measures

Annex 1: Technical and Organisational Measures

1. Confidentiality (Art. 32 para. 1 lit. b) GDPR) and encryption (Art. 32 para. 1 lit. a) GDPR)

Access control
Measures to prevent unauthorised persons from gaining access to the data processing systems used to process personal data:

Examples of possible precautions
- Entrance doors are always kept locked. - Visitors/external persons are accompanied or collected and supervised at all times. - Video surveillance with recording at the entrance door - Keys - Security service and/or security personnel at the entrance - Individual IT systems are operated in external data centres (hosting) and by external services (software-as-a-service). The respective provider guarantees access control there.

Access control/encryption
Measures that prevent unauthorised persons from using the data processing systems and procedures:

Examples of possible precautions
- Access to externally hosted/operated IT systems is specially secured (encryption) - Access to IT systems only possible with user ID and individual password - Access authorisations are documented. - Password policy is enforced on the mula platform. - IT systems are automatically locked in the event of repeated unsuccessful login attempts. - Functional assignment of individual end devices and logging of system usage - Mobile data carriers are encrypted (hardware encryption). - Screen lock on workstations, automatic locking in the event of prolonged absence - Two-factor identification

Access control
Measures to ensure that those authorised to use the data processing procedures can only access the personal data subject to their access authorisation:

Examples of possible precautions
- Individual access rights for each user (documented in a written authorisation concept), central administration and control - Access authorisations are granted on a task-related basis and according to the need-to-know principle. - Regular review of access authorisations. Authorisations that are no longer required are withdrawn immediately. - Recording of access to the IT system

Separation control / purpose limitation control
Measures to ensure that data collected for different purposes can be processed separately:

Examples of possible precautions
- Separation of clients on the software side - Separation of productive and test systems (in separate databases)

2. Integrity (Art. 32 para. 1 lit. b) GDPR)

Transfer control
Measures to ensure that personal data cannot be read, copied, altered or removed without authorisation during electronic transmission or during transport or storage on data carriers, and that it is possible to check and determine to which bodies personal data is to be transmitted by data transmission equipment:

Examples of possible precautions
- Data storage and processing takes place on IT systems in the data centre. Connection between clients and server is specially secured (encryption). - Bringing and using private data carriers is prohibited. Only encrypted company data carriers may be used. - Visitors have no access to the company LAN/WLAN.

Input control
Measures that ensure that it is possible to subsequently check whether and by whom personal data can be entered, changed or removed in data processing systems:

Examples of possible precautions
- Automated logging of data entry, modification or deletion - Logging of failed access attempts - Logging the activities of the system administrator and all users - Logging of all activities on the server - Protection of log data against loss or modification - Documentation of the input programmes

3. Availability and resilience (Art. 32 para. 1 lit. b) GDPR), rapid recoverability (Art. 32 para. 1 lit. c) GDPR)

Availability control
Measures to ensure that personal data is protected against accidental destruction or loss (the information relates to the Contractor's own IT systems):

Examples of possible precautions

- Data security concept
- Versioned data and system backups according to backup plan (daily/weekly)
- Backup computer centre
- Malware protection
- Security-relevant updates and patches are installed regularly and promptly.
- Reporting procedure and emergency plan
- Uninterruptible power supply

4. Procedures for regular review, assessment and evaluation (Art. 32 para. 1 lit. d) GDPR, Art. 25 para. 1 GDPR)

Processing control
Measures to ensure that personal data processed under contract can only be processed in accordance with the instructions of the Client:

Examples of possible precautions

- Contractors are carefully selected.
- Clear and unambiguous contractual provisions on data processing
- Control of the contractor by the management or the data protection officer.

Data protection management
Measures that enable data protection processes to be controlled and demonstrably ensure compliance with data protection regulations:

Examples of possible precautions

- A competent person has been appointed as data protection officer.
- Employees are regularly trained and sensitised to data protection and are instructed on the confidentiality of data.
- Employees have confidentiality clauses in their employment contracts